UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

4524 Newby Drive, Apartment G1, Durham, North Carolina 27704

Case No. 1:20mj65

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A(a)(2)(A)	Distribute/Receive Child Pornography
18 U.S.C. 2252A(a)(5)(B)	Possession with Intent to View Child Pornography

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

William Thompson | Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/28/20

Judge's signature

City and state: Greensboro, NC

L. Patrick Auld

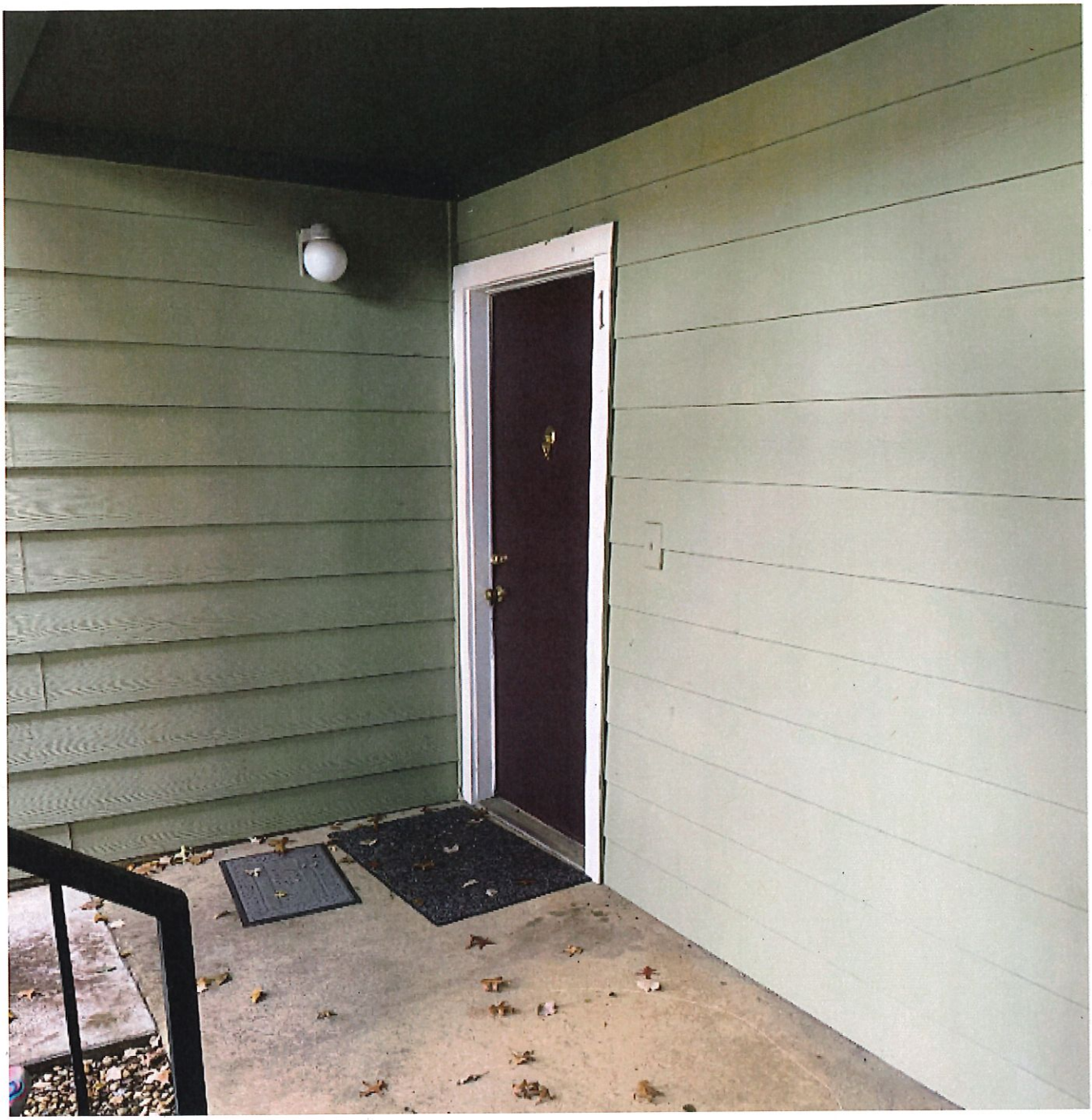
Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED ("SUBJECT PREMISES")

1. The entire premises located at 4524 Newby Drive, Apartment G1, Durham, North Carolina 27704 (the SUBJECT PREMISES) and any person located at the SUBJECT PREMISES found to be residing therein. The SUBJECT PREMISES is a one-story apartment on the first floor of a multi-unit apartment building within the Stonewood Apartment Homes community. The SUBJECT PREMISES is a grayish tone colored building with white trim and a shingled roof. The SUBJECT PREMISES, which is contained within a building bearing the letter "G" and the numerals "1-4,"

has a burgundy colored door with the numeral "1" posted on its white trim.



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8), and/or child erotica;
    b. Records, information, and items referencing or revealing the occupancy or ownership of 4524 Newby Drive, Apartment G1, Durham, North Carolina 27704, including utility and telephone bills, mail envelopes, or addressed correspondence;
    c. Records and information referencing or revealing access to and/or use of Kik Messenger;

d. Records and information referencing or revealing the use of the handle "ericbeal2222" or any variant thereof, and the identity of the user.

e. Records and information referencing or revealing the use of any handle that includes the phrase "ericbeal2222" and the identity of the user.

f. Records and information referencing or revealing the owner or user of an Apple iPhone smartphone;

g. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

h. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

i. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

j. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography; and

k. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

   b. evidence of how the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

   c. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;

   d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   e. evidence of the Internet Protocol addresses used by the COMPUTER;

   f. evidence of the times the COMPUTER was used;

   g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

   h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

   i. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

j. evidence of the lack of such malicious software;

k. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, William Thompson, a Special Agent ("SA") with Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the premises located at 4524 Newby Drive, Apartment G1, Durham, North Carolina 27704 (the "SUBJECT PREMISES"), more specifically described in Attachment A, and the person of Ernie BRINN for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment B.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§

2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES and on the person of Ernie BRINN.

AFFIANT BACKGROUND

3. I am a SA of the U.S. Department of Homeland Security (DHS), HSI, formerly the United States Customs Service, having been so employed since December 2001, and I am currently assigned to the HSI Raleigh office in Cary, North Carolina. While employed by HSI, I have investigated federal criminal violations related to high technology and cybercrime, child exploitation, and child pornography. I have received training from the Federal Law Enforcement Training Center (FLETC) and other law enforcement agencies in the areas of child exploitation and pornography investigations and pedophile behavior. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography. I have had the opportunity to observe and review numerous examples of child pornography as defined in 18 U.S.C. § 2256 in various forms of media, including computer media. In addition, I have participated in the execution of numerous search warrants involving child exploitation and child pornography offenses and I am in routine contact with

experts in the fields of computers, computer forensics and Internet investigations.

4. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce

by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where

(a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video

display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby- trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "Hash Value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic

sent from and directed to that computer or device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile Application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote Computing Service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually Explicit Conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "Storage Medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual Depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data

which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON KIK AND KIK REPORTS

7. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging. In October 2019, MediaLab, Inc., Santa Monica, California, purchased Kik from Ontario, Canada based Kik Interactive, Inc. According to the publicly available document "Kik's Guide for Law Enforcement,"[1] to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

8. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to

[1] Available at: https://lawenforcement.kik.com/hc/en-us/categories/200320809-Guide-for-Law-Enforcement.

communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

9. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik's Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik believes use of their services are in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images is critically important to protecting their users, product, brand, and business interests.

10. Upon receipt of the information and evidence precipitating this search warrant application, and contained herein, Kik was in Ontario, Canada, and governed by Canadian law. According to information contained in the "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" (hereinafter Kik Glossary), which Kik provided when reporting information to law enforcement authorities, Kik was mandated to report to the Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law which were discovered on the Kik platform. According to the Kik Glossary, Kik was typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third-party moderators.

11. According to the Kik Glossary, Kik was mandated to report any images and/or videos that would constitute suspected child pornography which are discovered on the Kik platform. Furthermore, according to the Kik Glossary, Kik is typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third-party moderators.

12. According to the Kik Glossary, Kik has developed an internal hash matching system called "SafePhoto" (similar to Microsoft's PhotoDNA system)

that Kik uses to scan images uploaded via Kik for suspected child pornography. Kik's SafePhoto database is comprised of hash values obtained from the International Criminal Police Organization (hereinafter "INTERPOL"), the RCMP and the National Center for Missing and Exploited Children (hereinafter "NCMEC"). Kik uses SafePhoto to run a hash value check against every image sent within Kik, including within private conversations, in order to detect images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When a user sends an image with a hash value that matches a child exploitation hash value in the SafePhoto database, Kik removes the content from its communications system, closes the user's account and provides a SafePhoto report of the incident to the RCMP.

13. The RCMP advised HSI agents that upon receiving a report from Kik related to suspected child pornography, the RCMP reviewed the reported IP addresses of the Kik users contained in the Kik Reports to determine their location. The RCMP then provided Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provided the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

PROBABLE CAUSE

Kik SafePhoto Report:

14. In October 2019, HSI Raleigh received a Kik SafePhoto report referral from the C3 CEIU concerning Kik user "ericbeal2222" who was reported for Child Sexual Abuse and Illegal Material (CSAM). Within this SafePhoto report, Kik documented "ericbeal2222" uploaded and sent a suspected image of child pornography through their group chat platform. Kik identified this image was uploaded by "ericbeal2222" on May 2, 2019, at 05:12:08 Universal Time Coordinated (UTC) utilizing IP address 174.109.70.153.

15. As part of this referral, HSI Raleigh received an image from the HSI Cyber Crimes Center (C3). HSI C3 documented they located this image in C3's National Child Victim Identification System (NCVIS) database and it's hash value matched the hash value of the image uploaded by Kik user "ericbeal2222" on May 2, 2019, at 05:12:08 UTC. I reviewed this image and verified it depicts child pornography showing a partially nude prepubescent female child. Within this image, the child is laying on her back on a carpeted floor and her right hand is touching her nude vaginal area which is positioned away from the camera. Also, at the fore of this image, a male's erect penis is visible and positioned on or near the child's left hand which she was holding on or near her mouth. In addition, a note reading, "I heart (a heart is drawn)

CUM" was written on pink paper/material and positioned behind the child's head.

16. As part of this SafePhoto referral, HSI Raleigh also received Kik subscriber records and user information for "ericbeal2222." These records revealed this user identified his name as "Eric Beal," his birth date as October 20, 1979, and an email address, ericbeal222@yahoo.com, annotated by Kik as unconfirmed[2] and deactivated. In addition, Kik documented "ericbeal2222" utilized an iPhone to access his account.

17. On November 4, 2019, HSI Raleigh submitted a DHS Summons to ISP Charter Communications requesting subscriber information for IP address 174.109.70.153 on May 2, 2019, at 05:12:08 UTC. Charter Communications responded and identified the subscriber, on the requested date and time, as Ernie Brinn at address 4524 Newby Drive, G1, Durham, North Carolina 27704 (SUBJECT PREMISES).

18. Subsequent public records database queries related to Eric BEAL and email address ericbeal222@yahoo.com failed to reveal any relevant results or linkages to the SUBJECT PREMISES and Durham, North Carolina.

[2] "Unconfirmed" means either that the email address is either invalid, or the user received a confirmation email from Kik but didn't click on the link to confirm.

19. On or about October 10, 2019, HSI Raleigh conducted queries of the North Carolina Division of Motor Vehicles (DMV) and discovered Ernie BRINN's (DOB: July 28, 1970) active North Carolina driver license. Review of BRINN's driver license, which is scheduled to expire on July 28, 2026, revealed he provided the SUBJECT PREMISES as his address.

20. On November 22, 2019, and January 17, 2020, I conducted vehicular surveillance and identified the SUBJECT PREMISES as a first-floor apartment in a multi-unit building. The SUBJECT PREMISES had a burgundy door with the numeral "1" posted on the white trim of the door. During surveillances, I observed a black Infiniti assigned North Carolina plate "ERNDOG," registered to Ernie BRINN at the SUBJECT PREMISES, parked in the lot directly outside of the SUBJECT PREMISES.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

21. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each

other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud"

storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*,

temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

22. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know the following are certain characteristics common to individuals who possess, receive and/or distribute child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual

media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are

valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[3]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

---

[3] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the individual utilizing Kik username "ericbeal2222," who is believed to be Ernie BRINN uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

23. Based on the following, I believe the user of "ericbeal2222" residing at the SUBJECT PREMISES likely displays characteristics common to individuals who possess, receive, distribute and/or maintain access with intent to view child pornography.

As detailed herein, the target of the investigation, "ericbeal2222" who is believed to be Ernie BRINN distributed child pornography via Kik. In order to distribute such materials, the user would necessarily have to acquire and possess child pornography.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

24. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to

literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these

purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

25. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES and on the person of Ernie BRINN, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. I submit that if a computer or storage medium is found at the SUBJECT PREMISES or on the person of Ernie BRINN, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years

after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES or on the person of Ernie BRINN because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows

investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

28. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer

equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

29. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic

examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence

described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

31. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the SUBJECT PREMISES described in Attachment A and on the person of Ernie BRINN. I respectfully request that this Court issue search warrants for the SUBJECT PREMISES described in Attachment A, and for the person of Ernie BRINN, authorizing the seizure and search of the items described in Attachment B.

William Thompson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 28th day of February 2019.

L. Patrick Auld
United States Magistrate Judge

has a burgundy colored door with the numeral "1" posted on its white trim.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8), and/or child erotica;
    b. Records, information, and items referencing or revealing the occupancy or ownership of 4524 Newby Drive, Apartment G1, Durham, North Carolina 27704, including utility and telephone bills, mail envelopes, or addressed correspondence;
    c. Records and information referencing or revealing access to and/or use of Kik Messenger;

d. Records and information referencing or revealing the use of the handle "ericbeal2222" or any variant thereof, and the identity of the user.

e. Records and information referencing or revealing the use of any handle that includes the phrase "ericbeal2222" and the identity of the user.

f. Records and information referencing or revealing the owner or user of an Apple iPhone smartphone;

g. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

h. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

i. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

j. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography; and

k. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

   b. evidence of how the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

   c. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;

   d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   e. evidence of the Internet Protocol addresses used by the COMPUTER;

   f. evidence of the times the COMPUTER was used;

   g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

   h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

   i. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

j. evidence of the lack of such malicious software;

k. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.